

الحمدلله معز الاسلام بنصره ومذل الشرك بقهره ومصرف الامور بأمره ومستدرج الكافرين بمكره الذي قدر الايام دولا بعدله وجعل العافية للمتقين بفضله والصلاة والسلام علي من أعلي الله منار الاسلام بسيفه وعلي اله وصحبه ومن تبعهم باحسان الي يوم الدين



مقالات أمنية

خدمات ال VPN

- ما معنى ال VPN ؟
- ما هي بروتوكولات الـVPNوما الفرق بينها ؟
- ما هي معايير امان خدمات ال VPN ؟
- هل خدمات الـVPNتغني عن استخدام شبكة تور؟
- ما افضل خدمات ال VPN التي تهتم بامن المستخدمين ؟



الصادرة عن مؤسسة آفاق الإلكترونية

Telegram.me/Horizons_lib



معظم الاخوة والاخوات يدركون ان كل خطوة علي شبكة الانترنت مسجلة ومراقبة كما وضحنا ذالك جليا في<u>سلسلة الحرب الإلكترونية وغفلة أنصار المجاهدين</u> ومن مميزات الـVPN انها تغير عناوين الIP والموقع الجغرافي وتشفر بيانات التصفح (Traffic) مما تحافظ علي خصوصيتك وتحميك من محاولات التعقب علي شبكة الانترنت ولكن يجب الانتباه الي ان كل خدمات الVPN ليست بمستوي امان واحد فبعض الخدمات تنتهك خصوصية المستخدمين وتشارك بياناتهم مع شركات الدعاية والاعلان او اجهزة الاستخبارات بغرض تعقبهم لذا ننصح الانصار بقراءة سياسة خصوصية وشروط استخدام اي خدمة VPN قبل استخدامها

مع الثورة التي احدثتها تسريبات إدوارد سنودن بأن وكالة الأمن القومي الامريكي حاولت لأعوام فك تشفير بروتوكولات خدمات الVPN فإن حقيقة ان معظم الخدمات التي تم تطويرها من قبل المعهد الوطني الامريكي للمعايير التقنية (NIST) يشتبه في اختراقها من قبل NSA لذا سنستعرض سلبيات وإيجابيات بروتوكولات التشفير التي تستخدمها شركات خدمات الVPN

ο ο ο ο ο ο ο ο ο ο ο ο ο ο ο

◇ ما معني الـ VPN ؟ ◇

ο ο ο ο ο ο ο ο ο ο ο ο ο ο ο



الـVPN هو إختصار لـVirtual Private Network وهي شبكة إتصال خاصة إفتراضية تقوم بتشفير بياناتك علي شبكة الانترنت وتمنع مزود الخدمة و الحكومات و الهكرز من تعقب نشاط المستخدمين مما يوفر للمستخدمين خصوصية وامان افضل اثناء التصفح

◇ بروتوكولات الـ VPN .. و الفرق بينها ◇

PPTPVPN

بروتوكول PPTP طور من قبل شركة مايكروسوفت بعام 1999 ثم اضافته الشركة بنظام Windows 95 و يعتمد علي اتصال بين نقطتين ويشفر البيانات بإستخدام خوارزمية RC4 بمفتاح 128 بت كحد أقصي يدعم كافة انظمة التشغيل ولكن اكتشفت به العديد من الثغرات الأمنية

[إيجابيات البروتوكول]

- **السرعة**
- **متوفر لجميع أنظمة التشغيل بشكل افتراضي**
- **سهل الإستخدام**

[سلبيات البروتوكول]

- **بروتوكول PPTP به العديد من الثغرات الأمنية ابرزها MS CHAPv2 authentication والتي مكنت وكالة الامن القومي الامريكي فك تشفير البيانات المشفرة من خلال البروتوكول ولا ننصح بإستخدامه تحت اي ظرف**

L2TP

بروتوكولL2TP/IPSEC مدعوم من معظم أنظمة التشغيل و متطور عن PPTP حيث يشفر البيانات باستخدام مفتاح AES-256 لم تكتشف به ثغرات أمنية حرجة بعد لكن طبقا لتسريبات ادوارد سنودن والتقرير الذي نشره الباحث الأمني John Gilmore فإن البروتوكول تم إضعافه اثناء مرحلة تصميمه مما اشار الي استطاعة وكالة الأمن القومي الأمريكي فك تشفير البيانات المشفرة ببروتوكول L2TP/IPSEC

[إيجابيات البروتوكول]

- **اكثر امانا من بروتوكول PPTP**

- سهل التثبيت على انظمة التشغيل
- مدعوم من قبل معظم انظمة التشغيل الحديثة
- أسرع من بروتوكول OpenVPN

[سلبيات البروتوكول]

- إضعاف البروتوكول اثناء مرحلة التصميم
- يمكن حظره من قبل الجدران النارية
- ربما استطاعت وكالة الأمن القومي الامريكي فك تشفيره (لا يوجد مصدر يوضح ذالك الى الان لكننا لا ننصح باستخدامه)



بروتوكول جديد مفتوح المصدر يستخدمOpenSSL library ويعد الافضل من بين البروتوكولات السابقة يستخدم مفتاح AES-256 بت ويدعم العديد من الخوارزميات مثل Blowfish , AES , 3DES , CAST-128 , Camellia لم يكتشف به اي ثغرات حرجة حتي الان ويعد الاقوي من بين البروتوكولات السابقة

[إيجابيات البروتوكول]

- سهولة التثبيت
- آمن جدا حيث لا يوجد اي دليل على استطاعة وكالة الأمن القومي الامريكي

- **يمكن تجاوز الجدران النارية من خلال بروتوكول OpenVPN**
- **يدعم نطاق واسع من خوارزميات التشفير**
- **مفتوح المصدر (اي يمكن فحصه وتحليله من قبل المتخصصين ولا يمكن اضافة باب خلفي للتجسس على المستخدمين فيه)**

[سلبيات البروتوكول]

- **يحتاج المستخدم الي تثبيت تطبيق من طرف ثالث (شركات الVPN)**
- **ابطئ من بروتوكول L2TP**

{ SSTP }

بروتوكول مقدم من قبل شركة مايكروسوفت في ويندوز Vista SP1 ومتاح الان لانظمة لينكس واجهزة الراوتر يستخدم البروتوكول SSLv3 ولذالك يتميز عن بروتوكول OpenVPN في بعض النقاط مثل القدرة علي استخدام منافذ TCP ك 443 لتجاوز مشاكل الحجب من قبل الجدران النارية لكن علي عكس OpenVPN فان بروتوكول SSTP مغلق المصدر ومطور من قبل شركة مايكروسوفت والتي لديها علاقات عميقة بوكالة الأمن القومي الامريكية

[إيجابيات البروتوكول]

- **يستخدم خوارزمية AES في تشفير البيانات**
- **يدعم جميع أنظمة ويندوز 7 , 8 , 8.1 , Vista**

- مدعوم من قبل شركة مايكروسوفت
- يستطيع تجاوز معظم الجدران النارية

[سلبيات البروتوكول]

- يعمل على انظمة ويندوز فقط
- مغلق المصدر ومقدم من قبل شركة مايكروسوفت مما لا يتيح للمطورين فحص الكود المصدري والتحقق من وجود ابواب خلفية او لا

{ IKEv2 }

بروتوكول جديد مبني علي البروتوكول السابق IPSEC ومطور من قبل شركة Microsoft و Cisco وقدم في نظام Windows 7 , البروتوكول مدعوم بشكل كبير من قبل أجهزة بلاك بيري كما يدعم انظمة لينكس (من خلال اضافات مفتوحة المصدر - نحن نعي ان اي شيئ مطور من قبل شركة مايكروسوفت فهو مصدر للشك لكن الاضافات مفتوحة المصدر اي يمكن تحليلها والتحقق من وجود ابواب خلفية او لا)

[إيجابيات البروتوكول]

- أسرع من بروتوكولات PPTP , SSTP L2P
- مستقر حيث يقوم باعادة الاتصال بشكل تلقائى عند انقطاعه على اجهزة بلاك بيري
- آمن حيث يستخدم خوارزميات AES-128 , AES-192 , AES-256 , 3DES
- سهل التثبيت
- يستخدم خاصية Perfect Forward Secrecy

[سلبيات البروتوكول]

- **غير مدعوم من كل انظمة التشغيل**
- **الاضافات المتوفرة لنظام لينكس فقط هي المفتوحة المصدر اي ان الاضافات المتوفرة لويندوز مغلقة المصدر ولا يمكن الوثوق بها**



◇ معايير امان خدمات الـ VPN ◇



بالطبع ليس كل خدمات الـ VPN امنة وتحافظ علي خصوصيتك كما يدعون ن هناك معايير يتم تقييم خدمة الـ VPN من خلالها يجب مراعاتها قبل استخدام ذه الخدمات وذالك من خلال قراءة سياسة خصوصية وشروط استخدام كل خدمة ما ننصح المناصرين بالتواصل مع الدعم الفني لخدمات الVPN للاستعلام ع النقاط الغير موضحة في سياسة الخصوصية وشروط الاستخدام مثل بروتوكو ت التشفير المستخدمة

❇ هل تُبقي شركة الVPN على أي سجلات لبياناتك ؟ إذا كان الأمر كذلك، م هي المعلومات التي تخزنها والي متي ؟

» **احذر الخدمات التي تحتفظ بسجلات المستخدم وتخزنها**

❇ ما الاختصاص الذي تعمل فيه الشركة المقدمة لخدمة الVPN ؟

» **يفضل اختيار الشركات التي تعمل بمجال الحماية الالكترونية لخبرتها في هذا مجال**

❇ هل تشارك بيانات المستخدمين (عنوان الIP والبريد الالكتروني) مع شركات الدع ة والا

» **ابتعد عن الخدمات التي تشارك بياناتك مع طرف ثالث (شركات الدعاية والاعلان و بما ج حكومية)**

❄ ما الخطوات التي ستقدم عليها الشركة اذا ما طلب منها بشكل قانوني تسليم بيانات احد مستخدمي خدمة الVPN ؟

» **احذر الخدمات التي تسلم بيانات المستخدمين الي الجهات الحكومية اذا ما طلب منها ذالك بشكل قانوني**

❄ هل تدعم خدمة Bit-Torrent والخدمات الاخري الخاصة بمشاركة الملفات وما الادوات التي تستخدمها الشركة في اعتراض اتصالات المستخدمين اذا ما اساءوا استخدام خدمة الVPN ؟

» **ان لم توضح خدمة الVPN ذالك تواصل مع الدعم الفني واسالهم عن الادوات ثم ابحث هل هذه الادوات تنتهك خصوصية المستخدمين**

❄ ما نظام الدفع المتاح وهل تقبل خدمة Bitcoin و Paypal وCASH U ؟

» **وجود نظام دفع امن امر ضروري لاي خدمة VPN حيث يتيح لك خصوصية وامان افضل من شراء الخدمة بالبطاقة البنكية مما قد يؤدي الي اعتقالك**

❄ ما خوارزمية التشفير التي تستخدمها ؟

» **تاكد ان خوارزمية التشفير المستخدمة AES -256**

❄ هل تستخدم الشركة سيرفرات للDNS خاصة بها ؟ ام تستخدم سيرفرات شركات طرف ثالث ؟

» **ابتعد عن الشركات التي تستخدم سيرفرات طرف ثالث**

❄ هل لديكم تحكم كامل في ادارة سيرفرات الVPN ؟ ام يتم ادارتها من قبل شركات طرف ثالث ؟

» **ابتعد عن الشركات التي لا تستطيع التحكم في ادارة سيرفرات الVPN بشكل كامل**

❄ ما هي البروتوكولات المدعومة في خدمة الVPN ؟

» **ننصح باستخدام بروتوكول OpenVPN**

○ ○

◇ هل خدمات الـ VPN تغني عن استخدام شبكة تور ◇

○ ○

سلسلة الوعي الأمني

مقارنة بين Tor وخدمات الـ VPN



:Tor

هو الجيل الثاني من نظام الموجهات البصلي . تم تطويره بمركز البحوث الامريكية ببداية الالفينات . ومن ثم تم اطلاقه علي شبكة الانترنت . تور الان تديره منظمة غير ربحية وغير حكومية NGO

:VPN

بروتوكولات الشبكات الخاصة الافتراضية تم تطويرها منذ بداية الثمانينات لتأمين اتصال الحكومات والمنظمات الحكومية . اول خدمة VPN بدات بمنتصف 1990 حيث تقدم خدمات الـ VPN شبكة امنة بين المستخدم والسيرفر

	Tor	VPN
مصدر التمويل	تعتمد شبكة تور بشكل اساسي علي تبرعات المستخدمين والمنظمات الخيرية والحقوقية في التمويل	معظم خدمات الVPN عبارة عن شركات خاصة المنظمات غير حكومية NGO
عدد العُقد	تتكون شبكة تور من ثلاث عقد (عقدة الدخول - العقدة الوسطى - عقدة الخروج)	تتكون الشبكات الخاصة الافتراضية من عقدة واحدة
عدد الخوادم (السيرفرات)	تحتوي شبكة تور علي اكثر من 6000 سيرفر	بعض الخدمات يصل عدد سيرفراتها من 10 الى 100 سيرفر حول العالم
عدد الموجهات داخل النظام (الموجهات Routers هي عملية نقل حزم البيانات من المستخدم الى الخوادم عبر شبكة الانترنت)	تعتمد الموجهات في شبكة تور علي عدد العقد حيث تحتوي شبكة تور علي اكثر من 1700 عقدة دخول و 1000 عقدة خروج و 2300 عقد وسطي فمن المحتمل انشاء 4 مليارات دائرة اتصال	يقدر عدد الموجهات في خدمات الشبكات الافتراضية بمئات قليلة
تغيير تردد الموجهات	كل تطبيق او برنامج يستخدم دائرة اتصال مختلفة عن الاخر وتتغير دائرة الاتصال بشكل تلقائي كل 10 دقائق علي شبكة تور	هذا يعتمد علي مزود الخدمة فمعظم خدمات الVPN يكون تغيير تردد الموجهات فيها بشكل يدوي ونادرا مايتم تغيير التردد بشكل تلقائي في خدمات الVPN
احتمالية استخدام موجهات استخدمتها من قبل	طبقا لوجود مليارات الموجهات بشبكة تور فان احتمالية استخدام موجه استخدمته من قبل قد تستغرق شهور او سنوات	طبقا لوجود عدد قليل من الموجهات بشبكة الVPN فان احتمالية استخدام موجه استخدمته من قبل قد يستغرق ايام او شهور قليلة
ما الذي يعرفه مزود الخدمة عنك ؟	يعرف انك تستخدم شبكة تور (يمكنك اخفاء ذالك من خلال استخدام الجسور في هذه الحالة لن يعرف مزود الخدمة انك تستخدم تور)	يعرف انك تستخدم خدمة VPN فقط لكن لا يستطيع معرفة ما المواقع التي تتصفحها او ماذا تفعل علي شبكة الانترنت
التخفي : من يعرف اكثر عنك ؟	شبكة تور تحتوي علي 3 عقد بدائرة الاتصال فجميع حزم البيانات يتم تشفيرها بين المستخدم لشبكة تور وبين عقدة الخروج لذا مديري عقد الخروج يستطيعون معرفة كل البيانات التي تمر بعقدة الخروج اذا لم تكن مشفرة ببروتوكول Https لكن عقدة الدخول فقط تعرف عنوان الIP الحقيقي لجهازك لكن عقدة الدخول لا تستطيع رؤية بياناتك التي تمر من خلال شبكة تور . العقد الوسطي تعزل عقدة الدخول عن عقدة الخروج فبالتالي يتم عزل عنوان الIP الحقيقي الخاص بك عن البيانات التي ترسلها من خلال شبكة تور	معظم خدمات الVPN تعرف عنوان الIP الخاص بك وتسجل البيانات التي ترسلها عبر شبكة الانترنت علي سيرفراتها وتقرا هذه البيانات لكن توجد خدمات VPN تحترم خصوصية المستخدمين ولا تنتهكها ولا تسجل بيانات علي سيرفرات الشركة او تقرأها
الامان والخصوصية: من يستطيع رؤية بياناتك والتحكم فيها؟	الاتصال بشبكة تور مشفر سواء من عقدة الدخول للعقدة الوسطي او من العقدة الوسطي لعقدة الخروج لكن يستطيع مديري عقد الخروج رؤية بياناتك اذا لم تستخدم بروتوكول التشفير Https اثناء تصفح المواقع وبروتوكول TLS في رسائل البريد الالكتروني	طالما خدمة الVPN تستخدم بروتوكول IPSEC او OPENVPN فلا يمكن لمزودي الخدمة معرفة ماتفعله علي شبكة الانترنت او رؤية بياناتك لان اتصالك مشفر لكن مزود خدمة الVPN يستطيع رؤية بياناتك مالم تستخدم بروتوكول HTTPS اثناء تصفح المواقع وبروتوكول TLS للبريد الالكتروني
سهولة الاستخدام	متصفح تور سهل في التعامل معه لكن المواقع التي تتصفحها من خلال متصفح تور فقط مشفرة اما اذا استخدمت اي خدمة اخري او برنامج اخر بعيدا عن متصفح تور لن يشفر اتصالك مالم تستخدم نظام Tails او Whonix	خدمات الشبكات الخاصة الافتراضية طريق بسيط وسهل للتخفي حيث تقوم خدمات ال VPN بتشفير كل اتصالك بالانترنت ولا يقتصر علي برنامج او متصفح بل كل البرامج بجهازك تستخدم شبكة الVPN
السرعة	شبكة تور تحتوي علي 3 عقد وتعتمد سرعة الاتصال علي قدرة العقدة علي تحمل كم البيانات والتبديل بين العقد مما يبطئ سرعة الاتصال بالانترنت	في الغالب خدمات الVPN سريعة جدا حيث تعتمد سرعة الخدمة علي بعد السيرفرات عن موقعك الحالي وحالة الشبكة
استنتاج	تور يعد افضل خيار للتخفي علي شبكة الانترنت طالما ضبطت اعداداته بشكل صحيح	خدمات الVPN خيار ممتاز للسرعة والحفاظ علي خصوصيتك لكن مستوي الحماية لخدمات الVPN لا يرقي الي التخفي علي شبكة الانترنت

○ ○

◇ افضل خدمات الـ VPN التي تهتم بامن المستخدم ◇

○ ○

يوجد العديد من الخدمات ولكن كل خدمة لها مميزات و عيوب طبقا للمعايير التي تم ذكرها وبناء علي هذه المعايير انصح باستخدام هذه الخدمات :

- NordVPN.com
- Mullvad.net
- IVPN.net
- hide.me
- FrootVPN.com
- AzireVPN.com
- *F-Secure freedome*

ونحذر.. **من استخدام بعض الخدمات الشائعة :**

- Hotspot Shield
- Strong VPN
- Avast Secure Line (يسجل بيانات المستخدمين لمدة30يوم واذا ماطلبت الجهات الحكومية منه بشكل قانوني بيانات المستخدمين سيسلمها)
- WI topia VPN
- Psiphon
- Surfeasy VPN
- Vypr VPN

وآخر دعوانا ان الحمد لله رب العالمين

ولا تنسوا اخوانكم من صالح الدعاء



للدعم الفني تواصل معنا على

| **SR444TAW** |**Tech Support**